IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412101

AGRO-TRUST!!- An Agriculture Product Supply Chain Management using Blockchain, IOT.

Kalyan Ram P S[1], Mrs Preeja Mary R[2], Ganne Rahul Naidu[3], Mohammed Ameen[4], Tarun K[5]

Department of Information Science and Engineering, The Oxford College of Engineering,

Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[1-5]

Abstract: Counterfeiting and supply chain inefficiencies, especially in the agricultural sector, lead to major safety risks and eco nomic losses. Traditional tracking systems using barcodes, RFID, or centralized databases remain vulnerable to manipulation and lack full transparency. This paper presents AGRO-TRUST!!, a platform integrating Blockchain, IoT, cloud computing, and cyber security to ensure secure and real-time traceability. Each product receives a blockchain-linked QR code, while IoT sensors such as GPS, MQ gas sensors, and DHT11 modules continuously record environmental and location data throughout the logistics cycle. Smart contracts automate secure payment procedures and product verification, while cloud computing enables scalable data processing and connection. Strong cyber security measures prevent manipulation and unauthorized access, such as encryption and role-based access control. 99.5% integrity in IoT data transmission and immediate identification of counterfeit efforts employing cloned QR codes are demonstrated by experimental results. AGRO-TRUST!! offers a transparent, tamper-proof, and scalable solution for agricultural and related supply chains.

Keywords: Blockchain, Internet of Things (IoT), Supply chain, smart contracts, blockchain, IoT, QR codes, and counterfeit detection

I. INTRODUCTION

Data manipulation, ineffective product traceability mechanisms, and the widespread circulation of counterfeit goods continue to intensify the global supply chain crisis. These challenges directly affect consumer trust, organizational credibility, and public safety across multiple sectors, including electronics, pharmaceuticals, agriculture, and food distribution. According to international trade analyses, counterfeit goods constitute more than 3% of global trade, resulting in yearly economic losses of billions of dollars and putting customers' health and safety at grave danger. These difficulties are made worse by the lack of openness and the simplicity with which product information can be fabricated. In the agricultural sector, these problems manifest in the form of contaminated food products, improper post-harvest handling, and the absence of efficient systems that track produce from farm to market. Many suppliers, farmers, and transporters still rely on centralized ERP systems or manual documentation, which are vulnerable to intentional falsification, illegal manipulation, and data loss. People are left wondering about the origin, quality, and, as a result, Furthermore, competition from inferior or fake goods often results in financial losses for reputable businesses. Furthermore, product spoilage, shortened shelf life, and higher operating expenses across the supply chain are all caused by the absence of real time environmental monitoring.

Although traditional identification technologies such as bar codes, RFID tags, and QR-coded serial systems provide partial automation, they fall short in ensuring complete authenticity and traceability. These systems depend heavily on centralized databases that are vulnerable to hacking, duplication, unauthorized access, and single-point failures. Counterfeiters can easily clone barcodes or replicate RFID tags, making it difficult for stakeholders to differentiate genuine products from fake ones. Furthermore, traditional methods do not support continuous monitoring of critical environmental parameters—including temperature, humidity, gas levels, and geographic location—which are essential in sensitive supply chains like agriculture, pharmaceuticals, and perishable goods.

The lack of unchangeable, tamper-proof records is another significant disadvantage. Stakeholders may become suspicious of centralized systems since they can be changed without leaving any evidence. It becomes difficult to identify sites of failure, assign responsibilities, and guarantee product integrity throughout the supply chain lifecycle It is deficient decentralized and transparent process for documenting every transaction, handoff, or environmental change. These limitations highlight the urgent need for an integrated, secure, and intelligent supply chain framework that combines real-time IoT sensing, trustworthy data storage, automated verification, and strong cybersecurity. Emerging technologies such as blockchain and cloud computing show great potential in addressing these gaps by offering decentralized record keeping, high scalability, and resilient system architectures.

II. PROBLEM STATEMENT AND OBJECTIVE

The global supply chain ecosystem continues to face persistent challenges such as data manipulation, circulation of counterfeit products, limited transparency, and fragmented information flow across stakeholders. Consumer goods, pharmaceuticals, and agriculture are among the industries that are greatly impacted by these problems, as product authenticity, quality, and traceability are essential for both safety and legal compliance. Vulnerable identifying technology like barcodes and RFID tags, centralized databases, and handwritten record keeping are the mainstays of current supply chain management systems. While these methods provide basic tracking, they are prone to replication, unauthorized modification, single-point failures, and data tampering. As a result, verifying product authenticity and maintaining stakeholder trust becomes difficult, particularly in complex, multi-stage logistics networks.

Consumer goods, pharmaceuticals, and agriculture are among the industries that are greatly impacted by these problems, as product authenticity, quality, and traceability are essential for both safety and legal compliance. Vulnerable identifying technology like barcodes and RFID tags, centralized databases, and handwritten recordkeeping are the mainstays of current supply chain management systems. Furthermore, the absence of real-time environmental data during storage and transit prevents timely interventions, resulting in reduced product quality and increased wastage. These draw backs underscore the necessity of an intelligent, transparent, and secure system that can offer automated validation, end-to end traceability, and real-time product status monitoring.

The following are the goals of the recommended system to deal with them issues:

- Use blockchain technology to guarantee product trace ability and ensure tamper-proof recording of transactions across the supply chain.
- Incorporate IoT sensors such as temperature, humidity, and GPS modules for real-time monitoring of environ mental and logistical conditions.
- Provide QR-based verification mechanisms for customers, retailers, and distributors to authenticate products instantly and reliably.
- Implement smart contracts to automate validation pro cesses, ownership transfers, and secure financial transactions.
- Enforce strong cybersecurity measures and leverage cloud-based analytics to ensure data integrity, scalability, and secure multi-party communication.

III. SCOPE

This research focuses on the design, implementation, and evaluation of an integrated blockchain- and IoT-enabled framework for agricultural supply chain management, named AGRO-TRUST!!. The scope of the study is limited to improving transparency, traceability, data integrity, and counterfeit detection across multi-stage agricultural supply chains.

The system enables end-to-end product traceability by tracking agricultural products from the point of origin through storage, transportation, and retail distribution to the final consumer. Each product batch is digitally registered and associated with a unique blockchain-linked QR code, ensuring tamper-proof identification and verifiable provenance throughout its lifecycle. The study incorporates IoT-based environmental monitoring using sensors such as DHT11 for temperature and humidity measurement, MQ-series gas sensors for spoilage detection, and GPS modules for location tracking. These devices collect real-time environmental and location data during storage and transportation to assess product quality and detect deviations that may indicate spoilage, mishandling, or tampering.

The scope also includes the integration of smart contracts on an Ethereum-compatible blockchain to automate critical supply chain operations such as product registration, ownership transfer, environmental violation logging, and counterfeit detection. Blockchain technology ensures immutability, decentralization, and trust among multiple stakeholders. To support scalability and real-time analytics, the framework leverages cloud computing for data aggregation, preprocessing, visualization, and off-chain storage of high-frequency sensor data. Cloud services act as an intermediary between IoT devices, blockchain networks, and web applications, enabling efficient data flow and continuous system availability.

The study further addresses cybersecurity and access control by implementing encryption techniques, role-based access control, JWT-based authentication, and secure API communication to protect sensitive data and prevent unauthorized access across all system layers.

DOI: 10.17148/IJARCCE.2025.1412101

The experimental scope includes evaluating the reliability of IoT data transmission, the performance of smart contracts, the accuracy of QR code–based counterfeit detection, and the overall usability of the system for farmers, transporters, retailers, and consumers. The scope of this work is limited to a prototype-level implementation and does not include large-scale commercial deployment, long-term field testing, or advanced AI-based predictive analytics, which are identified as potential directions for future enhancement.

IV. LITERATURE REVIEW

[1] Nikkhah et al. (2020) analyzed IoT-based smart farming frameworks and showed that IoT significantly improves real-time monitoring, automation, and decision-making in agriculture. However, the study lacks integration with cloud platforms and blockchain, limiting scalability, secure data storage, and end-to-end traceability.
[2] Kamilaris et al. (2018) studied blockchain applications in agriculture and highlighted improvements in transparency, traceability, and trust among stakeholders. The work also identified major limitations such as high energy consumption, transaction latency, and scalability issues associated with public blockchain networks.
[3] Li et al. (2020) proposed a Blockchain–IoT–Cloud architecture that enables real-time product tracking and data sharing across supply chain stages. Despite improved traceability, the system faced performance bottlenecks and scalability challenges when processing large volumes of IoT sensor data.
[4] Ferrag et al. (2020) focused on strengthening security in IoT-based agricultural systems by introducing encryption, authentication, and access control mechanisms. However, the absence of blockchain integration limits data immutability and decentralized trust.
[5] Lin et al. (2021) demonstrated that cloud computing enhances agricultural monitoring, analytics, and data accessibility. At the same time, the study emphasized concerns related to data privacy, centralized control, and vulnerability to cyberattacks in cloud environments.
[6] Tripathi et al. (2022) developed a blockchain-IoT-based supply chain system using smart contracts to reduce logistics fraud and automate verification processes. The study noted that high deployment and operational costs restrict its adoption at large scale.
[7] Tan et al. (2022) and Reyna et al. (2018) proposed hybrid blockchain-IoT-cloud architectures that improve system security, transparency, and trust. Their studies also reported challenges such as increased latency, limited IoT device processing power, and integration complexity.
[8] Sharma et al. (2021) proposed a multi-layer cybersecurity framework for smart farming focusing on intrusion detection and authentication mechanisms. However, the work lacks real-world deployment validation and practical performance evaluation in live agricultural environments.
[9] Wang et al. (2021) reviewed blockchain-based agricultural supply chain systems and concluded that blockchain improves data integrity and traceability. However, the study pointed out challenges related to interoperability, transaction throughput, and integration with real-time IoT sensor data.
[10] Menon and Iyer (2023) explored blockchain-supported food supply chain traceability and observed improved quality assurance and consumer trust. The work highlighted limitations such as high infrastructure costs and the lack of standardized frameworks for large-scale agricultural deployment.

4.1 Gaps or Areas for Improvement

The majority of current solutions are still insufficient, un duly domain-specific, or technologically dispersed despite the increasing use of blockchain and IoT, cloud computing, and cybersecurity in agricultural and industrial supply chains has been the subject of numerous studies. Numerous significant research gaps have been noted, including:

- Absence of Unified Frameworks: The majority of earlier research concentrates on specific technologies, such blockchain for record-keeping or IoT for sensing, without offering an integrated, end-to-end framework that com bines the layers of cybersecurity, cloud, blockchain, and IoT for total traceability.
- Limited Integration of Real-Time Data: While many blockchain-based systems capture static product data, they neglect to integrate continuous, real-time IoT sensor feeds (such as GPS, temperature, humidity, and gas levels), They are necessary for perishable goods and agriculture.
- Problems with scalability and latency: Public blockchains, are not appropriate for high-frequency Internet of Things data or large agricultural settings due to high gas costs and transaction delay.
- Lack of Security and Privacy Mechanisms: Despite multiple studies' recommendations for authentication and encryption, few systems handle multi-layer cybersecurity across cloud infrastructure, blockchain transactions, and IoT devices, leaving them open to data breaches.
- Lack of Standardization and Interoperability: Current solutions sometimes rely on closed cloud systems or proprietary hardware, which restricts cross-platform communication and interoperability among various stakeholders (consumers, distributors, retailers, and farmers).

DOI: 10.17148/IJARCCE.2025.1412101

V. SYSTEM ARCHITECTURE

The system architecture of the AGRO-TRUST!! project is designed to provide secure, transparent, and real-time monitoring of agricultural products across the entire supply chain. The working of the system follows a structured flow of data from physical sensing to digital verification, ensuring authenticity, traceability, and data integrity at every stage. The process starts at the IoT sensing layer, where sensors are deployed at farms, storage units, and transportation vehicles. The DHT11 sensor continuously measures temperature and humidity to monitor environmental conditions that directly affect product quality. MQ gas sensors detect the presence of harmful or spoilage-related gases, helping to identify contamination or deterioration at an early stage. GPS modules collect real-time location data, enabling continuous tracking of product movement throughout the logistics process.

All sensor readings are collected by the NodeMCU microcontroller in the communication layer. The NodeMCU aggregates data from multiple sensors, timestamps the readings, and performs basic preprocessing such as noise filtering and range validation. After preprocessing, the data is transmitted securely to the backend server using Wi-Fi or GSM connectivity, ensuring reliable and uninterrupted communication between the physical devices and the digital system. The backend processing layer is implemented using a Spring Boot–based server hosted on the cloud. This layer receives incoming sensor data and performs detailed validation, storage, and analysis. Sensor data and product metadata are stored in cloud databases for real-time monitoring and historical reference. The backend continuously evaluates sensor values against predefined threshold limits. When abnormal conditions such as temperature deviations, gas level increases, or route anomalies are detected, alerts are generated and prepared for permanent recording.

Blockchain integration is achieved through smart contracts that are triggered by the backend during critical events. These smart contracts record immutable information such as product registration details, ownership transfers, environmental condition violations, and location updates. Since blockchain records are decentralized and tamper-proof, once data is written it cannot be altered, ensuring transparency and trust among all supply chain participants.

During product registration, a unique QR code linked to the blockchain record is generated and attached to the physical product or batch. This QR code serves as the digital identity of the product. At any point in the supply chain, stakeholders can scan the QR code using the mobile application to retrieve verified information related to origin, handling conditions, transportation history, and current status. If the scanned data does not match the blockchain record, the system flags the product as counterfeit or tampered.

The user interface layer is provided through a mobile application that offers role-based access to farmers, transporters, retailers, and consumers. Farmers can register products and monitor environmental conditions, transporters can track logistics and sensor updates, retailers can verify authenticity during receiving, and consumers can confirm product quality and origin before purchase. The application communicates securely with the backend using authenticated APIs to ensure confidentiality and controlled access.

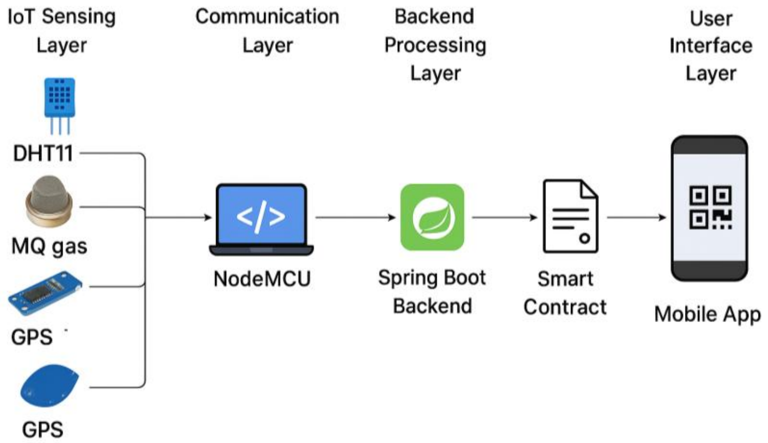


Figure 1: System Architecture

Overall, the layered system architecture enables seamless integration of IoT sensing, secure communication, cloud-based backend processing, blockchain smart contracts, and user-facing applications. This working mechanism ensures real-time traceability, counterfeit detection, and secure data management across the agricultural supply chain, making the system reliable, scalable, and practical for real-world deployment.

DOI: 10.17148/IJARCCE.2025.1412101

VI. METHODOLOGY

The implementation approach employs a systematic workflow to construct, launch, and verify a protected blockchain-IoT distribution network framework for merchandise monitoring and fraud mitigation. The process initiates with requirement specification and system architecture planning, progressing to hardware implementation for environmental parameter and geographic position detection. Sensor information transmits through microcontroller units to a Spring Boot application layer, which authenticates data inputs and records them through Ethereum programmable contracts onto the distributed ledger. Distinctive QR identifiers connect products to these permanent records, facilitating stakeholder interaction interfaces. Validation procedures encompass data verification, counterfeit identification algorithms, and real-time notification systems for anomalies or interference, unifying hardware components, software infrastructure, and blockchain technology for dependable complete-cycle functionality.

6.1 Hardware Specification

The platform employs Arduino Uno and NodeMCU (ESP8266) microcontrollers for information acquisition and communication within blockchain-supervised distribution networks. Arduino Uno functions as the primary sensor integration point, connecting DHT11 climate monitors (thermal and moisture parameters), MQ atmospheric detectors, GPS positioning units, precipitation sensors, and soil hydration monitors to capture live environmental and geographic intelligence indicating degradation, interference, or improper handling. GPS modules deliver precise coordinate data for movement documentation.

NodeMCU manages wireless network connectivity, acquiring structured sensor information (format: temp#humi#mq#lat#lon) from Arduino through UART serial communication protocols. It transforms data into JSON format and transmits HTTP POST requests to backend infrastructure for blockchain recordation. This bifurcated microcontroller architecture segregates sensing operations (Arduino) from network transmission (NodeMCU), guaranteeing efficient, dependable data transfer.

6.2 Software Specification

The system architecture implements layered software components for information management, distributed ledger communication, and stakeholder interfaces:

- **Spring Boot (Java Application Layer):** Constructs RESTful API endpoints for item enrolment, QR identifier creation, sensor data interpretation, and blockchain integration. Delivers scalability, protection mechanisms, and function-based access control for network participants.
- **Arduino C/C++ (Sensor Programming):** Develops Uno firmware for live measurement acquisition utilizing libraries including DHT.h, TinyGPS++, and SoftwareSerial.h. Consolidates information for serial transmission to NodeMCU.
- **NodeMCU Firmware (ESP8266 C/C++):** Implements ESP8266WiFi and HTTPClient libraries to interpret serial inputs, structure JSON payloads, and transmit POST requests to Flask/server interfaces.
- **Flask (Python Processing Layer):** Accepts NodeMCU transmissions, extracts measurement values, eliminates signal interference, and routes to backend/blockchain infrastructure for authentication.
- **Android Java (Mobile Interface):** Delivers QR scanning capabilities (ZXing/ML Kit integration) and API connectivity to present provenance records, activity logs, and authentication status for immediate verification.
- **Web3.py (Python Blockchain Interface):** Establishes Ethereum network connections for smart contract invocation, transaction authentication, and data commitment operations.
- **Solidity (Programmable Contracts):** Executes on Ethereum for product enrolment, custody transfers, event documentation, and QR-blockchain associations, guaranteeing permanent transaction records.

Summary of Software Stack

Layer	Technology	Purpose
Backend Server	Java Spring Boot	Product management, REST APIs, QR generation, blockchain interaction
IoT Firmware	Arduino C/C++	Sensor reading & serial data generation
Wi-Fi Communication	NodeMCU C/C++	Send JSON data to Flask server
Data Receiver API	Python Flask	Accept sensor data and pass to blockchain/backend
Mobile Application	Android Java	QR scan, product verification UI
Blockchain API	Python Web3.py	Smart contract integration
Smart Contracts	Solidity	Immutable product tracking and authenticity logic

DOI: 10.17148/IJARCCE.2025.1412101

VII. IMPLEMENATION ENVIRONMENT

The implementation environment of the proposed system is designed to create a fully integrated and cohesive framework that combines IoT, backend services, blockchain, and user-facing applications to enable a robust, scalable, and reliable supply chain monitoring solution. At the core of the hardware environment are IoT devices, including NodeMCU (ESP8266) microcontrollers, DHT11 temperature and humidity sensors, MQ series gas sensors, and GPS modules. These devices work collaboratively to collect real-time environmental and positional data, which is crucial for monitoring agricultural products during storage and transportation.

The sensors are interfaced directly with the NodeMCU, which functions as the central processing unit. It reads sensor outputs, performs basic preprocessing such as filtering or averaging the data, and transmits the information over Wi-Fi networks. The low-power operation of the IoT devices ensures that the system can function continuously in field conditions or moving vehicles without significant energy constraints, which is critical for long-term monitoring in rural and transportation settings.

On the software side, the IoT devices are programmed using the Arduino IDE with embedded C/C++, taking advantage of standard libraries for sensor interfacing, Wi-Fi communication, and data formatting. The software ensures smooth operation and stable communication between the hardware and backend systems. Secure communication protocols, such as HTTPS or MQTT over TLS, are implemented to ensure that sensor data transmitted over wireless networks is encrypted and resistant to interception, preserving data integrity and confidentiality.

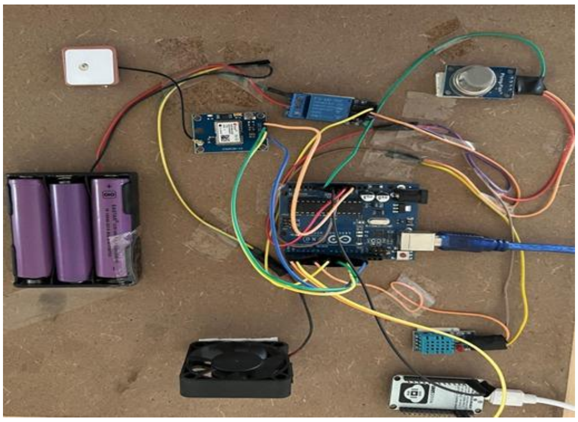
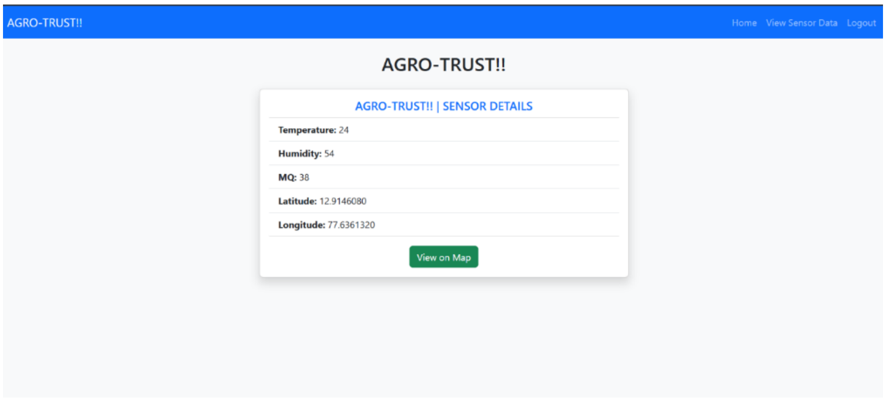


Figure 2: Hardware prototype showing Arduino uno with MQ, GPS, DHT 11, ESP8266 NodeMCU Board.

The backend environment forms the backbone of the system, developed using Java and the Spring Boot framework. This layer provides RESTful APIs that allow IoT devices, mobile applications, and web interfaces to interact seamlessly with the server. The backend is responsible for authentication, authorization, role-based access control, data validation, and executing the business logic that governs product traceability, transaction processing, and monitoring rules. A cloud-hosted database, such as MySQL or MongoDB, is used to store sensor logs, user information, product details, and transaction records. This database structure ensures fast retrieval, secure storage, and scalability to accommodate growing datasets as the system expands.



AGRO-TRUST!!

AGRO-TRUST!! | SENSOR DETAILS

Temperature: 24

Humidity: 54

MQ: 38

Latitude: 12.9146080

Longitude: 77.6361320

Figure 3: Live Sensor Data from Sensors Pulled from Blockchain through Remix, Ganache and Python Web3.0

Blockchain technology is integrated as a decentralized layer to maintain tamper-proof records of critical supply chain information. A private or consortium blockchain network is used, and smart contracts are deployed to automate processes like product registration, ownership transfers, and traceability logging. These smart contracts enforce rules in a transparent and immutable manner, ensuring that once data is recorded, it cannot be altered without proper authorization. The backend communicates with the blockchain layer through secure APIs, allowing only verified and authenticated transactions to be recorded, thereby enhancing the reliability and trustworthiness of the system.

The frontend environment includes mobile and web applications developed using frameworks like React for web interfaces or Android Studio for mobile apps. These applications provide user-friendly interfaces tailored to different stakeholders, such as farmers, transporters, retailers, and end consumers. Users can interact with the system to scan QR codes on products, track real-time location and environmental conditions, verify product authenticity, and access complete traceability histories. The frontend is designed to offer intuitive navigation, clear visualization of data, and responsive performance across devices.

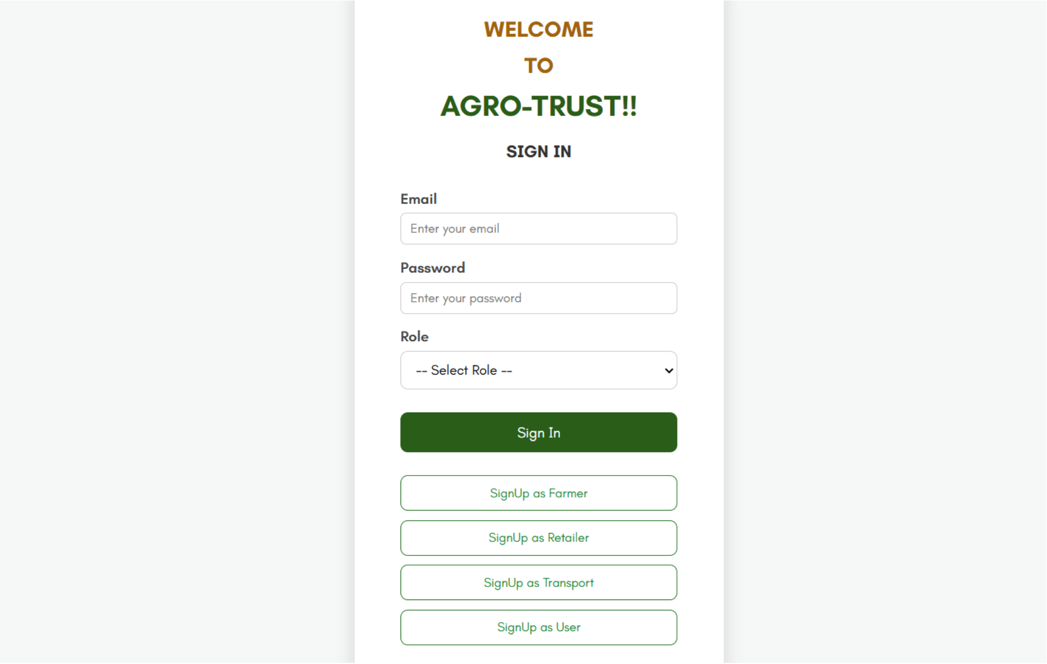
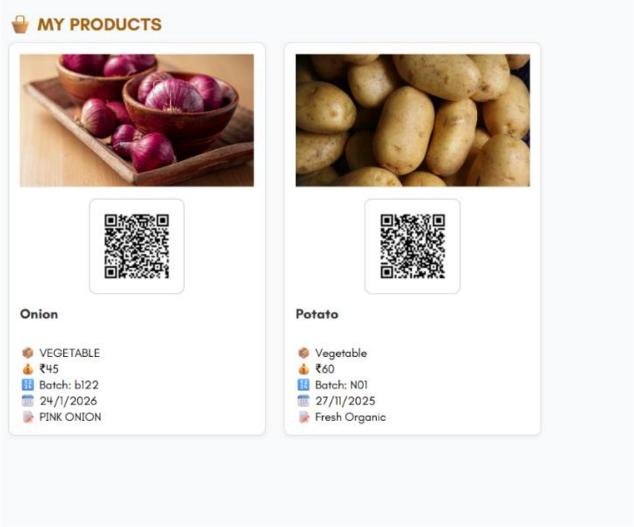


Figure 4: Software – Home Page



Onion

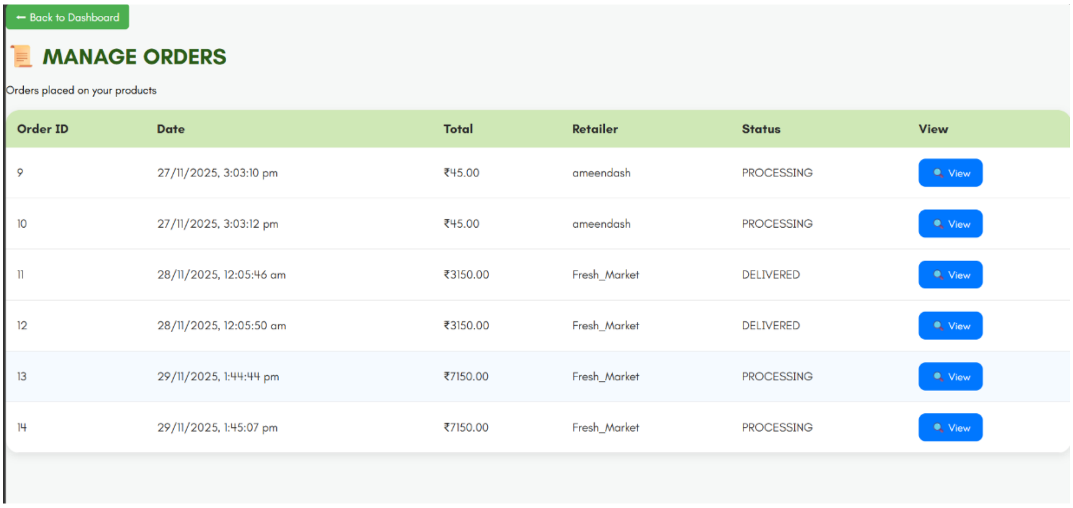
📦 VEGETABLE
💰 ₹45
🔢 Batch: b122
📅 24/1/2026
📝 PINK ONION

Potato

📦 Vegetable
💰 ₹60
🔢 Batch: N01
📅 27/11/2025
📝 Fresh Organic

Figure 5: Software – Products Page from Farmer Portal

DOI: 10.17148/IJARCCE.2025.1412101

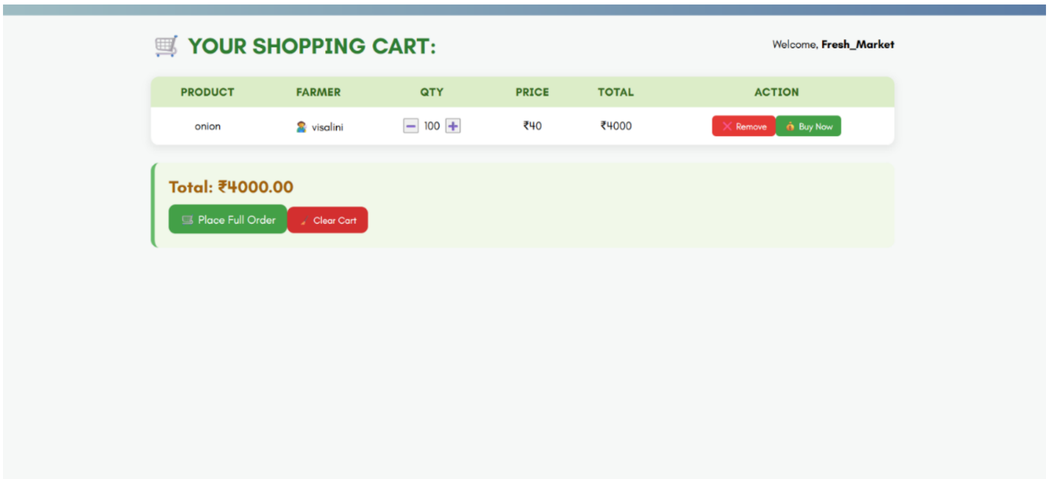


MANAGE ORDERS

Orders placed on your products

Order ID	Date	Total	Retailer	Status	View
9	27/11/2025, 3:03:10 pm	₹45.00	ameendash	PROCESSING	View
10	27/11/2025, 3:03:12 pm	₹45.00	ameendash	PROCESSING	View
11	28/11/2025, 12:05:46 am	₹3150.00	Fresh_Market	DELIVERED	View
12	28/11/2025, 12:05:50 am	₹3150.00	Fresh_Market	DELIVERED	View
13	29/11/2025, 1:44:44 pm	₹7150.00	Fresh_Market	PROCESSING	View
14	29/11/2025, 1:45:07 pm	₹7150.00	Fresh_Market	PROCESSING	View

Figure 6: Software – Orders Page from Farmer Portal

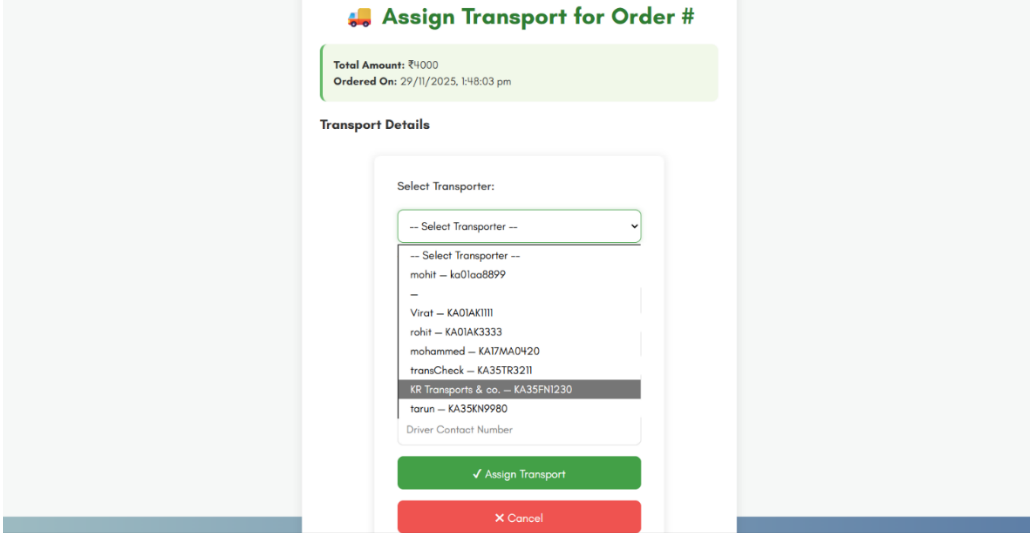

YOUR SHOPPING CART:

Welcome, **Fresh_Market**

PRODUCT	FARMER	QTY	PRICE	TOTAL	ACTION
onion	visalini	− 100 +	₹40	₹4000	Remove Buy Now

Total: ₹4000.00

Figure 7: Software – Cart Page from Retailer Portal


Assign Transport for Order #

Total Amount: ₹4000
Ordered On: 29/11/2025, 1:48:03 pm

Transport Details

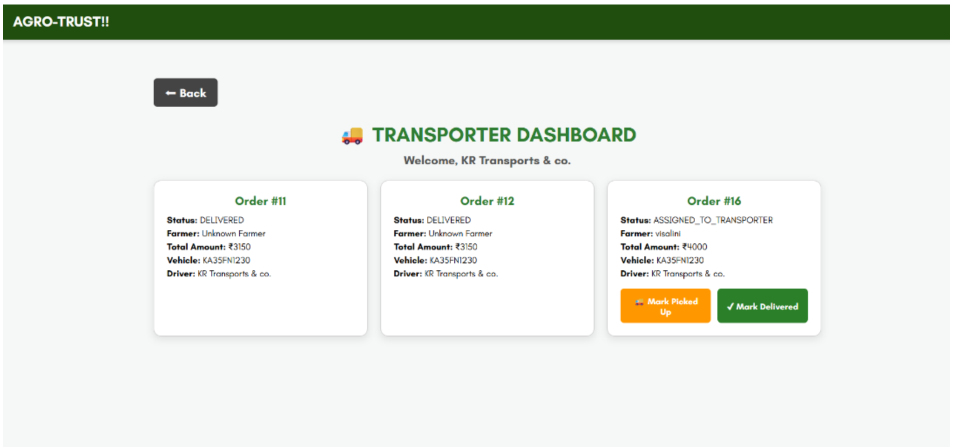
Select Transporter:

-- Select Transporter --

-- Select Transporter --
mohit – ka01aa8899
–
Virat – KA01AK1111
rohit – KA01AK3333
mohammed – KA17MA0420
transCheck – KA35TR3211
KR Transports & co. – KA35FN1230
tarun – KA35KN9980

Figure 8: Software – Transporter Assigning Page from Farmer Portal

DOI: 10.17148/IJARCCE.2025.1412101



🚚 TRANSPORTER DASHBOARD

Welcome, KR Transports & co.

Order #11

Status: DELIVERED
Farmer: Unknown Farmer
Total Amount: ₹3150
Vehicle: KA35FN1230
Driver: KR Transports & co.

Order #12

Status: DELIVERED
Farmer: Unknown Farmer
Total Amount: ₹3150
Vehicle: KA35FN1230
Driver: KR Transports & co.

Order #16

Status: ASSIGNED_TO_TRANSPORTER
Farmer: visalini
Total Amount: ₹4000
Vehicle: KA35FN1230
Driver: KR Transports & co.

Figure 9: Software – Transporter Dashboard Page from Farmer Portal

Finally, the deployment environment leverages cloud infrastructure to host backend services, databases, and potentially parts of the blockchain network. Cloud deployment ensures high availability, load balancing, and the capacity to scale resources as the number of users or IoT devices increases. Additional measures such as continuous monitoring, logging, backup mechanisms, and basic cybersecurity protections are implemented to maintain system reliability, ensure data security, and provide uninterrupted service for all users. Overall, this integrated environment enables real-time, end-to-end traceability, providing transparency, efficiency, and trust across the entire agricultural supply chain.

VIII. MODULES

The proposed system is divided into several interrelated modules, each designed to perform specific functions within the overall supply chain monitoring and traceability framework. These modules work together to ensure seamless data collection, secure storage, and efficient retrieval of information for all stakeholders.

1. IoT Data Collection Module: This module is responsible for capturing real-time environmental and positional data from agricultural products. IoT devices, including NodeMCU (ESP8266), DHT11 temperature and humidity sensors, MQ gas sensors, and GPS modules, are deployed in storage units, transport vehicles, and fields. The NodeMCU acts as the primary controller, reading sensor outputs, performing preliminary data preprocessing, and transmitting the data securely to the backend. This module ensures continuous monitoring of product conditions such as temperature, humidity, gas levels, and location, which is critical for maintaining product quality and safety throughout the supply chain.

2. Backend Processing and Management Module: The backend module, developed using Java and the Spring Boot framework, handles data reception, storage, and processing. It provides RESTful APIs for communication with IoT devices and frontend applications. The backend is responsible for authentication, role-based access control, data validation, and business logic execution, ensuring that only authorized users can perform specific actions. It also manages product registration, transaction records, and historical sensor logs in a cloud-hosted database like MySQL or MongoDB, enabling efficient retrieval and analytics for decision-making.

3. Blockchain and Smart Contract Module: This module ensures the integrity, transparency, and immutability of supply chain data. A private or consortium blockchain network is employed, with smart contracts deployed to manage product registration, ownership transfers, and traceability records. Each critical action is recorded on the blockchain, preventing unauthorized modifications and providing a reliable audit trail. The backend communicates with this module through secure APIs, ensuring that only verified and accurate data is stored on the blockchain ledger.

4. User Interface Module: The frontend module includes mobile and web applications designed for different stakeholders, including farmers, transporters, retailers, and consumers. Developed using frameworks such as React for web applications or Android Studio for mobile apps, this module allows users to interact with the system easily. Users can scan QR codes, track products in real-time, verify authenticity, and access detailed traceability histories. The interface emphasizes usability, responsive design, and clear visualization of critical information.

5. Deployment and Monitoring Module: This module focuses on deploying the system on cloud infrastructure to ensure high availability, scalability, and reliability. Continuous monitoring, logging, and security measures are applied to detect

anomalies, maintain system performance, and protect sensitive data. It ensures uninterrupted access to services and supports the dynamic scaling of resources as the number of IoT devices and users increases.
.

IX. PERFORMANCE EVALUATION

The performance evaluation of the proposed system focuses on assessing its efficiency, reliability, scalability, and overall effectiveness in managing real-time supply chain traceability. Various metrics are considered to ensure that the system operates optimally under different conditions, including continuous monitoring in agricultural fields, transportation units, and retail environments.

9.1 Introduction to Testing Approach

To ensure that this Blockchain-IoT infrastructure truly functions dependably and securely in practical settings, testing is crucial. To determine whether each component is functioning effectively both separately and collectively, the entire system made up of the IoT sensors that monitor the items, customers must be viewed as a single system. Our testing strategy will incorporate a number of approaches and strategies to evaluate simultaneously. Unit testing evaluates how components, such as sensor accuracy or API call functionality, work. Integration testing guarantees that information sent, won't be lost or corrupted. System testing identifies the vulnerabilities of the systems under realistic circumstances, such as altered sensor readings, unexpected network disconnections, weak GPS signals, and even penetration attempts to see. In order to validate that the interfaces are, in fact, user-friendly and that the needs of many participants are being satisfied, we also conduct stakeholder acceptance testing. Security testing prioritizes evaluating data dependability, smart contract execution, and the system's ability to thwart unauthorized access attempts. The accuracy, reaction of the backend are assessed. Blockchain technology adheres to a lengthy and stringent testing methodology to guarantee data consistency, transaction permanence, and contract logic execution as intended. Real-world usability testing is done concurrently for mobile applications', and interface design because the system wouldn't work if consumers couldn't utilize it easily. Combining all of the aforementioned criteria results in a robust, scalable, and secure platform that can track products and identify fakes using user-friendly, frustration-resistant interfaces.

Test Cases

This is a comprehensive list take into account the main components of the system, which include the mobile application, backend services, hardware sensors, and blockchain capabilities. In order to guarantee the overall dependability of the system, the tests are designed to identify flaws. On the hardware side, some sensors are utilized that activate and continue to function throughout the duration of a product's trip.

1. IoT Hardware Sensor Testing

Test Case ID	Test Situation	Input	Anticipated Results	Real Outcome	Status
HW-TC01	Temperature and humidity reading	DHT11 sensor connected	Correct temperature and humidity values	Values displayed on serial monitor	Pass
HW-TC02	Gas sensor reading	Exposure to smoke/gas	MQ sensor detects high values	Relay turns ON/OFF based on threshold	Pass
HW-TC03	Soil and rain sensor reading	Wet soil / dry soil	Analog values mapped 0–100%	Correct percentage displayed	Pass
HW-TC04	GPS location accuracy	Outdoor environment	GPS lock obtained	Latitude & longitude printed	Pass
HW-TC05	Arduino → NodeMCU communication	Sensor data from UNO	Complete data string via Serial	NodeMCU receives correctly	Pass

DOI: 10.17148/IJARCCE.2025.1412101

2. NodeMCU Wi-Fi and API Communication Testing

Test Case ID	Scenario	Input	Expected Output
NC-TC01	Wi-Fi connection	Correct SSID & password	NodeMCU connects successfully
NC-TC02	JSON formatting	Sensor data string	Formed JSON → {"data":"temp#humi#mq#lat#lon"}
NC-TC03	POST request	JSON to Flask API	HTTP 200 response with success message
NC-TC04	Network failure handling	Wi-Fi off	Retry connection message
NC-TC05	Server down handling	Wrong Flask URL	HTTP error with proper logging

3. Backend Spring Boot API Testing

Test Case ID	Scenario	Input	Expected Output
SB-TC01	Valid POST request	Correct JSON	API stores data & returns success
SB-TC02	Missing fields	Partial JSON	Error response with validation message
SB-TC03	Database storage test	Insert sensor record	Record saved with timestamp
SB-TC04	Fetch product history	QR code ID	Complete blockchain + IoT history sent
SB-TC05	High traffic test	Multiple requests/sec	System responds without crashing

4. Blockchain Integration and Smart Contract Testing

Test Case ID	Scenario	Input	Expected Output
BC-TC01	Product registration	Product ID	New blockchain entry added
BC-TC02	Data immutability	Modify previous block	Modification rejected
BC-TC03	Valid sensor update	Correct payload	New block transaction recorded
BC-TC04	Tampering attempt	Fake sensor data	Smart contract triggers alert
BC-TC05	QR verification	QR scan	Displays original blockchain history

5. QR Code and Android Application Testing

Test Case ID	Scenario	Input	Expected Output
APP-TC01	QR scan	Valid QR	Product details retrieved
APP-TC02	QR scan	Fake QR	“Counterfeit product” warning
APP-TC03	History display	Product ID	Timeline + sensor values shown
APP-TC04	API timeout	No server response	“Server unreachable” message
APP-TC05	UI responsiveness	User navigation	No lag, smooth operations

6. System Integration Testing

Test Case ID	Scenario	Input	Expected Output
INT-TC01	Full cycle	Sensor → NodeMCU → Flask → Spring Boot → Blockchain → Android	End-to-end transmission successful
INT-TC02	Real-time variation	Changing sensor values	Live updates visible in backend
INT-TC03	Supply chain update	Changing owner	Blockchain logs new owner
INT-TC04	Counterfeit simulation	Manually altered data	System detects mismatch
INT-TC05	GPS movement	Change device location	Live location updates stored

DOI: 10.17148/IJARCCE.2025.1412101

7. Non-Functional Validation

Performance Metrics

- API endpoint response duration < 2 seconds
- Distributed ledger transaction completion < 5 seconds
- Mobile application data retrieval < 3 seconds

Security Measures

- Unauthenticated QR identifier scan → restricted information visibility
- SQL injection attempts → blocked through input sanitization
- Blockchain record tampering → prevented through architectural design

User Experience

- Mobile application intuitive navigation structure
- All interface elements accessible and comprehensible
- Streamlined scanning workflow for end-users

System Stability

- Platform maintains functionality despite sensor reading variations
- Automatic network reconnection upon Wi-Fi interruption

X. CONCLUSION

Integrating advanced sensor technology with blockchain's secure record-keeping creates a trustworthy end-to-end tracking solution that is hard to deceive or alterThroughout the course of the product's lifecycle, the process depends on sensors that are continuously running and integrated into the hardware. While MQ sensors detect particular gases to identify contamination or degradation caused by poor storage. GPS modules offer accurate position tracking, guaranteeing that stakeholders are constantly aware of the products' presence.

The blockchain permanently records all of the data gathered by these sensors, protecting it from manipulation and. Because transactions are logged throughout the whole in a susceptible central database, the system's decentralized architecture further improves security by guaranteeing resilience and integrity along the supply chain. Every product engagement, every sensor reading, every ownership transfer, etc., become part of an everlasting record that cannot be changed or erased without mathematical proof. Smart contracts are mainly the ones that take care of the automation of the routine tasks like new product registration, ownership transfer, sensor data validation, and counterfeit warning activation. The mechanization of these processes minimizes the chance of human error occurring as well as eliminating the possibilities of fraud while at the same time guaranteeing the uniformity of business rules implementation throughout the whole network.

The technical architecture employs Spring Boot for the smooth management of APIs, Python for the smart processing of sensor data, and Web3py for the connection of all components to the blockchain. Such elements collaborate to ensure that data is continuously synchronized and also to provide verification functionalities all over the system. However, what is more significant is that the system offers powerful tools to all the stakeholders. Consumers are able to utilize very user-friendly Android applications or web portals for scanning QR codes and immediately getting a complete verified history of a product. Retailers, shipping companies, and manufacturers have also got the same easy and quick access to the authentication data, which in turn establishes trust and aids every party in making better and more informed decisions regarding the products they are dealing with or are about to buy. The system is functioning in numerous industrial sectors that are facing problems of counterfeiting and quality acceptance.

Agricultural supply chains can track produce from farm to table, ensuring freshness and authenticity. Pharmaceutical companies can verify medications haven't been tampered with or replaced with dangerous fakes. Electronics manufacturers can protect against counterfeit components that might fail or cause safety issues. Consumer goods companies get better control over their products, and food distributors can monitor conditions throughout the cold chain to prevent spoilage. Beyond just catching fakes, the platform supports ethical sourcing and sustainability efforts while cutting the enormous financial losses that counterfeiting causes every year.

The design is intentionally flexible and modular, which means we can add new capabilities as technology evolves. Future enhancements could include AI algorithms that spot unusual patterns and flag potential problems before they escalate. We're looking at combining cloud computing's power with edge processing to make the system even faster and more responsive. Multi-language support will make it accessible in different markets worldwide. Permissioned blockchain options could improve performance for enterprise deployments where companies want more control over who participates. And tighter integration with regulatory frameworks will help businesses stay compliant with evolving laws and standards across different countries.

6.2 Future Enhancements

We've identified several exciting directions to take our product authentication and counterfeit detection platform forward. Here's what we're considering:

Smarter Systems Through AI: We're looking at bringing in artificial intelligence to help us understand what the IoT sensors are telling us. The solution wasn't just to gather data but to detect indicators of badness for instance when a product was nearing the end of its life cycle or when there was something suspicious in the supply chain. To put it simply, preventing complications from occurring through prompt detection and that was the whole point of the system along with better decision-making all round.

Balancing Speed and Power: Presently, we are looking at a configuration that does part of the data processing at edge and then does the heavy lifting in the cloud. Imagine a scenario where a smart assistant is doing some instantaneous tasks on the spot and sending the complex ones to the main office. All of this translates to quicker reactions, reduced expenses, and a network with lower load, including the situation of blockchain transactions that are still cheap.

Speaking Everyone's Language: Global usage of this platform is only possible if it operates properly for people in all regions. This implies that the development of applications and interfaces in multiple languages must be accompanied by the adaptations for the different ways of doing things in particular areas. Directly, we are considering farm workers and labourers who do not understand English but have to operate the platform daily.

Smarter Blockchain Choices: Public blockchains may become costly and move at a slow pace. We are pondering over a consortium model where only authenticated partners would be allowed to participate. It is quicker, less expensive, and provides companies with the privacy controls they require without compromising on security.

Playing Nice with Regulators: Think of a situation where our blockchain goes on communicating straight with the government departments and certifying bodies. The process of auditing would become more uncomplicated, the adherence to regulations would be through the system, and the whole system would have more trust from all stakeholders. Regulatory checks could even be carried out within the smart contracts so that the approvals would be faster and less documentation would be required.

Contracts That Adapt: Business rules change. Regulations evolve. We want to build smart contracts that can be updated without breaking everything. It's like being able to renovate your house while still living in it—the system keeps running while we make improvements.

Better Ways to See What's Happening: Dashboards and alerts are required that are really understandable to people. Monitors of products are the producers, while the carriers would want to monitor their shipments and the regulators require tools for supervision. Good visualization allows all to detect the problems fast and then choose wisely.
Beyond Food and Consumer Goods: The fundamental tech is applicable in any industry that is concerned about counterfeit drugs, electronics, luxury products, etc. Venturing into these fields implies that we will be able to safeguard a larger number of individuals, provide more advantages, and continue the technological advancement.

Connecting Different Blockchain Networks: Eeventually, distinct corporations and nations may adopt dissimilar blockchain infrastructures. We are considering the communication between them all so that a product certified in one network can be believed in another. That is the way we construct a genuinely international authentication system. All these concepts indicate one direction: the creation of a solution that is capable of adapting to the requirements of businesses and customers, outsmarting counterfeiters, and being beneficial to people globally.

ACKNOWLEDGMENT

The authors thank the faculty and staff of the Department of Information Science and Engineering at The Oxford College of Engineering for their advice and assistance. We are grateful to the open-source communities that support Python Web3.0, Remix, and Ganache as well as to **Mrs. Preeja Mary R**. for her technical advice and mentoring.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412101

REFERENCES

[1]. T. Tian, "An Internet of Things, blockchain, and HACCP-based supply chain traceability solution for food safety," in Proc. Int. Conf. Service Syst. Serv. Manage. (ICSSSM), Kunming, China, 2017, pp. 1–6.

[2]. T. Toyoda, K. Matheny, Z. Zheng, R. K. Iyer, and K. M. T. Fan, "A Product Ownership Management System (POMS) built on blockchain to prevent counterfeit goods," in Proc. IEEE Int. Conf. Consumer Electron. (ICCE), Las Vegas, NV, USA, 2017, pp. 138–139.

[3]. A. Sylim, C. Liu, M. Zheng, and S. Choi, "Blockchain technology for detecting falsified and substandard pharmaceuticals," J. Med. Syst., vol. 42, no. 8, pp. 1–12, 2018.

[4]. F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification, and open issues," Telemat. Inform., vol. 36, pp. 55–81, 2019.

[5]. H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," Intell. Syst. Account. Finance Manag., vol. 25, no. 1, pp. 18–27, 2018.

[6]. M. Kouhizadeh and J. Sarkis, "Blockchain practices, potentials, and perspectives in greening supply chains," Sustainability, vol. 10, no. 10, pp. 1–25, 2018.

[7]. J. Leng, P. Zhou, X. Liu, and Y. Xu, "Blockchain-empowered sustainable manufacturing and product lifecycle management: A survey," J. Manuf. Syst., vol. 56, pp. 1–14, 2020.

[8]. K. Francisco and D. Swanson, "The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency," Logistics, vol. 2, no. 1, pp. 1–10, 2018.

[9]. A. Rejeb, J. G. Keogh, and K. Treiblmaier, "Leveraging the Internet of Things and blockchain technology in supply chain management," Future Internet, vol. 11, no. 7, pp. 161–182, 2019.

[10]. S. Patel, "Blockchain and IoT-enabled food traceability system for agricultural supply chains," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 2, pp. 1–8, 2023. give me 10 more references

[11]. M. Casino, A. Dasaklis, and C. Patsakis, "Blockchain-based food supply chain traceability: A review of benefits and challenges," Comput. Ind., vol. 125, pp. 103334, 2021.

[12]. Y. Wang, M. Li, and H. Zhang, "Blockchain-based data integrity and traceability for agricultural supply chains," Comput. Electron. Agric., vol. 179, pp. 105849, 2020.

[13]. S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," Int. J. Prod. Res., vol. 57, no. 7, pp. 2117–2135, 2019.

[14]. L. Tian, J. Li, and Y. Chen, "A blockchain-based traceability system for agricultural products," IEEE Access, vol. 8, pp. 113389–113402, 2020.

[15]. A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, "The rise of blockchain technology in agriculture and food supply chains," Trends Food Sci. Technol., vol. 91, pp. 640–652, 2019.

[16]. S. Kim, Y. Park, and J. Lee, "IoT-based smart agriculture system integrated with blockchain," Sensors, vol. 20, no. 23, pp. 1–18, 2020.

[17]. R. Casado-Vara, J. Prieto, F. De la Prieta, and J. M. Corchado, "Blockchain framework for IoT data quality via edge computing," Future Gener. Comput. Syst., vol. 98, pp. 874–885, 2019.

[18]. A. Rejeb, K. Rejeb, and J. G. Keogh, "Digital transformation of agriculture supply chains using blockchain and IoT," Technol. Forecast. Soc. Change, vol. 162, pp. 120385, 2021.

[19]. M. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 5G and IoT-based smart agriculture: Challenges and solutions," Comput. Netw., vol. 179, pp. 107451, 2020.

[20]. P. Tsang, Y. Wu, and K. Chen, "Smart contract-based secure traceability system for agri-food supply chains," IEEE Trans. Eng. Manag., vol. 69, no. 4, pp. 1281–1294, 2022.